



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/735,509	12/12/2003	Sudarshan Palliyil	JP920030270US1	5856
39903	7590	04/03/2007	EXAMINER	
ANTHONY ENGLAND PO Box 5307 AUSTIN, TX 78763-5307			TURCHEN, JAMES R	
			ART UNIT	PAPER NUMBER
			2139	
SHORTENED STATUTORY PERIOD OF RESPONSE	MAIL DATE	DELIVERY MODE		
3 MONTHS	04/03/2007	PAPER		

Please find below and/or attached an Office communication concerning this application or proceeding.

If NO period for reply is specified above, the maximum statutory period will apply and will expire 6 MONTHS from the mailing date of this communication.

Office Action Summary	Application No.	Applicant(s)
	10/735,509	PALLIYIL ET AL.
	Examiner	Art Unit
	James Turchen	2139

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --
Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) Responsive to communication(s) filed on 12 December 2003.
 2a) This action is FINAL. 2b) This action is non-final.
 3) Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) Claim(s) 1-23 is/are pending in the application.
 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
 5) Claim(s) _____ is/are allowed.
 6) Claim(s) 1-23 is/are rejected.
 7) Claim(s) _____ is/are objected to.
 8) Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) The specification is objected to by the Examiner.
 10) The drawing(s) filed on 12 December 2003 is/are: a) accepted or b) objected to by the Examiner.
 Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
 Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
 11) The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
 a) All b) Some * c) None of:
 1. Certified copies of the priority documents have been received.
 2. Certified copies of the priority documents have been received in Application No. _____.
 3. Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- | | |
|---|---|
| 1) <input checked="" type="checkbox"/> Notice of References Cited (PTO-892) | 4) <input type="checkbox"/> Interview Summary (PTO-413) |
| 2) <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948) | Paper No(s)/Mail Date. _____ |
| 3) <input checked="" type="checkbox"/> Information Disclosure Statement(s) (PTO/SB/08)
Paper No(s)/Mail Date <u>12/12/2003</u> . | 5) <input type="checkbox"/> Notice of Informal Patent Application |
| | 6) <input type="checkbox"/> Other: _____ |

DETAILED ACTION

1. Claims 1-23 are pending.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

The factual inquiries set forth in *Graham v. John Deere Co.*, 383 U.S. 1, 148 USPQ 459 (1966), that are applied for establishing a background for determining obviousness under 35 U.S.C. 103(a) are summarized as follows:

1. Determining the scope and contents of the prior art.
2. Ascertaining the differences between the prior art and the claims at issue.
3. Resolving the level of ordinary skill in the pertinent art.
4. Considering objective evidence present in the application indicating obviousness or nonobviousness.

This application currently names joint inventors. In considering patentability of the claims under 35 U.S.C. 103(a), the examiner presumes that the subject matter of the various claims was commonly owned at the time any inventions covered therein were made absent any evidence to the contrary. Applicant is advised of the obligation under 37 CFR 1.56 to point out the inventor and invention dates of each claim that was not commonly owned at the time a later invention was made in order for the examiner to consider the applicability of 35 U.S.C. 103(c) and potential 35 U.S.C. 102(e), (f) or (g) prior art under 35 U.S.C. 103(a).

Claim 1 is rejected under 35 U.S.C. 103(a) as being unpatentable over Nachenberg (US 6,021,510) in view of Nachenberg et al. (US 5,765,030) and Glover (6,763,466).

Nachenberg discloses computing a set of hash values representing a set of resources (column 4 lines 5-8); in response to a requirement for a virus check (column 4 lines 23-27, the file is being examined (scanned) a subsequent time), comparing the computed hash values to identify resources within said set of resources having matching hash values (column 4 lines 40-47); performing a virus scan for a first resource within said set of resources (column 4 lines 48-57, examiner interprets that virus scanning comprises the act of comparing the hash values as well as other known scanning techniques). Nachenberg does not disclose recording a virus-free or contaminated status for the first resource or the identified resources that are the same as the first resource. Nachenberg et al. discloses tagging a file as virus-free or contaminated or infected according to whether or not the scan identifies a virus (column 3 lines 4-9). It would have been obvious to one of ordinary skill in the art at the time of invention to combine the anti-virus method of Nachenberg with the tagging method of Nachenberg et al. in order to identify if a file is contaminated in order to quarantine, clean the infected file, or prevent a file from being executed. Glover discloses the use of caching for the anti-virus state for files that have been scanned during recent executions of the anti-virus program (column 1 lines 56-66, this would mark files with the same parameters as virus-free or contaminated to avoid the need for a full scan of the file). It would have been obvious to one of ordinary skill in the art at the time of

invention to combine the method of Nachenberg and Nachenberg et al. with the caching system of Glover in order to determine that a virus scan is not necessary (column 1 line 63).

Claims 2 and 5 are rejected under 35 U.S.C. 103(a) as being unpatentable over Nachenberg, Nachenberg et al, and Glover as applied to claim 1 above, and further in view of Albrecht (US 2001/0005889).

Nachenberg, Nachenberg et al, and Glover disclose the method of claim 1, comparing hash values, performing a virus scan, and recording a virus-free or contaminated status, but they do not disclose a first data processing system within the network or disinfecting the file and forwarding the disinfected file to the data processing systems. Albrecht discloses receiving the copy of the resource at the first data processing system (figure 3, agent returns file portions, paragraph 0048) and performing a virus scan of resource at the scanning engine (paragraph 0048). Albrecht additionally discloses disinfecting the file (paragraph 0049) and forwarding it to the agent. It is inherent in a data processing system, such as a database, to update all files that are identical to a file that has changed as to maintain integrity of the database as a whole. It would have been obvious to one of ordinary skill in the art at the time of invention to combine the method disclosed by Nachenberg, Nachenberg et al, and Glover with the centralized scanning engine of Albrecht in order to reduce maintenance overheads for the anti-virus applications (paragraph 003).

Claim 3 is rejected under 35 U.S.C. 103(a) as being unpatentable over Nachenberg, Nachenberg et al. and Glover as applied to claim 1 above, and further in view of Feigen et al. (US 2002/0138554).

Nachenberg, Nachenberg et al. and Glover disclose the method of claim 1, but they do not disclose computing the hash value at a remote node in the network. Feigen et al. discloses the method wherein the host hashes a block of code (figure 2, 202), transmits parameters to client (204), the remote device hashes and determines hash value (206 and 208), and sends the hash to host for comparison by host (210 and 212). In paragraph 0016, Feigen et al. discloses that if the two hash values are identical, the host confirms that the code at the resident has not been tampered with. Feigen et al. discloses that if the two hashes are not identical, then the host may take additional action. It would have been obvious to one of ordinary skill in the art at the time of invention to combine the hash sending method of Feigen et al. with the anti-virus and hashing method of Nachenberg, Nachenberg et al., and Glover in order to verify the integrity of software associated with a plurality of remote network appliances served by the network host (Feigen et al, paragraph 008).

Claim 4 is rejected under 35 U.S.C. 103(a) as being unpatentable over Nachenberg, Nachenberg et al, Glover, and Albrecht as applied to claim 2 above, and further in view of Arnold et al. (US 5,440,723).

Nachenberg, Nachenberg et al, Glover, and Albrecht disclose the method of claim 2, but they do not forward an indication of the virus-free or contaminated status to a plurality of data processing systems at which a resource matching the first resource

is stored. Arnold et al. discloses sending a virus indication to neighboring systems (column 19 line 64 to column 20 line3). It would have been obvious to one of ordinary skill in the art at the time of invention to modify the virus indication with a virus-free or contaminated indication and to combine the notification method of Arnold et al. with the method disclosed in claim 2 in order to notify neighboring computers (column 19 lines 46-48).

Claims 6-9 and 19-21 are rejected under 35 U.S.C. 103(a) as being unpatentable over Radatti (US 7,143,113) in view of Nachenberg et al. (US 5,765,030).

Radatti discloses receiving a set of hash values derived by applying a secure hash function to each of a set of resources and storing a set of hash values (column 3 lines 39-41 show using a MD5 hash; column 3 lines 44-48 show the hash values can be stored internally or externally). Radatti further discloses comparing the computed hash values to identify resources within said set of resources having matching hash values (column 5 lines 53-55 show finding duplicates by matching hash values) and performing a virus scan (column 6 lines 17-22 shows scanning for known hash values of Trojan horses, trap doors, back doors, etc.). Radatti discloses using the identification of replicated resources to generate a report of the distribution of replicas of a resource (column 5 lines 59-60 shows forming a report of the results). Radatti does not disclose recording a virus-free or contaminated status or recording the status for identified resources having the same hash values. Nachenberg et al. discloses tagging a file as virus-free or contaminated (column 3 lines 4-9). It would have been obvious to one of ordinary skill in the art at the time of invention to combine the method for hashing and

Art Unit: 2139

recording hashes of Radatti with the method for tagging a file as virus-free or contaminated of Nachenberg et al. in order to identify which files are virus-free or contain viruses. Additionally, it would have been obvious to one of ordinary skill in the art at the time of invention to notify all resources with the same hash value (identical files) in order to avoid unnecessary virus scanning of identical files (saving time and computational cycles).

Claims 10 and 11 are method claims for controlling performance of an operation and are anticipated by the same rejection as claims 1-9 as a virus scan is an operation.

Claims 12, 13, 17, and 22 are rejected under 35 U.S.C. 103(a) as being unpatentable over Radatti in view of Nachenberg et al.

Radatti discloses a data processing unit (column 3 lines 8-12, controlling computer systems), a data storage unit (column 3 lines 8-12, storage media), a repository manager configured to store a set of hash values in at least one repository within the data storage unit (column 3 lines 44-48), wherein the set of hash values are derived from a set of resources determined to be virus-free or contaminated (column 4 lines 31-34, the scope of the security system in full would produce hash values for those files that are determined to be virus-free as well as those determined to have a virus, column 6 lines 17-48 disclose checking for known virus hashes). Radatti discloses using the identification of replicated resources to generate a report of the distribution of replicas of a resource (column 5 lines 59-60 shows forming a report of the results). Radatti does not disclose a virus scan coordinator (or a coordinator for performance of an operation) for performance of a virus scan determining that the first resource is virus-

free or contaminated by controlling the repository manager to record a virus-free or contaminated status in association with the first resource and resources having hash values matching the hash value of the first resource. Nachenberg et al. discloses tagging a file as virus-free or contaminated (column 3 lines 4-9). It would have been obvious to one of ordinary skill in the art at the time of invention to combine the method for hashing and recording hashes of Radatti with the method for tagging a file as virus-free or contaminated of Nachenberg et al. in order to identify which files are virus-free or contain viruses. It is inherent that anti-virus programs have a scheduler or manager (coordinator) that will scan files on access (in real time) or as scheduled (Nachenberg et al. column 1 lines 21-24). It would have been obvious to one of ordinary skill in the art at the time of invention to notify all resources with the same hash value (identical files) in order to avoid unnecessary virus scanning of identical files (saving time and computational cycles). Claim 13 discloses the use of a coordinator for coordinating performance of an operation (a virus scan is an operation) and is therefore rejected under the same reasoning as above.

Claims 14-16 are rejected under 35 U.S.C. 103(a) as being unpatentable over Radatti and Nachenberg et al. as applied to claim 13 above, and further in view of Hoefelmeyer et al. (US 7,043,757).

Radatti and Nachenberg et al. disclose the data processing apparatus of claim 13, but they do not disclose a plurality of operator programs, each configured to respond to instructions from the coordinator to perform a respective operation in relation to the first resource. Hoefelmeyer et al. discloses multiple virus scanners running in

parallel (column 3 lines 31-44). A virus scanner is an operator program so a virus scanner anticipates an operator program. It is inherent that antivirus programs contain decontamination code; therefore multiple virus scanners would contain multiple virus-decontamination programs. It would have been obvious to one of ordinary skill in the art at the time of invention to combine the data processing apparatus of Radatti and Nachenberg et al. with the multiple virus scanners of Hoefelmeyer et al. in order to reduce the latency of scanning a file (column 2 lines 35-38).

Claims 18 and 23 correspond to the computer program of the system disclosed in claims 12, 13, and 22 and are therefore rejected by the same reasoning as claims 12, 13, and 22.

Conclusion

The prior art made of record and not relied upon is considered pertinent to applicant's disclosure. Cited prior art discloses virus scanning and file integrity methods and systems.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to James Turchen whose telephone number is 571-270-1378. The examiner can normally be reached on MTWRF 7:30-5:00.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on 571-272-3795. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

JRT

Taghi T. Arani
Primary Examiner
Taghi T. Arani
3/30/04